



#20/
E
BH
6-24-01

UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: COLLINS et al. Atty Docket No: 20206-25 (PT-TA 410 (Cont 1))
Serial No: 09/328,726 Group Art Unit: 2131
Filing Date: October 26, 1998 Examiner: Leaning, J.
For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

Box No Fee Amendment
Assistant Commissioner for Patents
Washington, D.C. 20231

RECEIVED
JUN 21 2001
Group 2100

AMENDMENT

Sir:

In response to the Office Action mailed on April 2, 2001, Applicants respectfully request reconsideration of the above-identified patent application. Please amend the above identified application as follows and consider the following remarks.

In The Claims:

1 14. (Three Times Amended) A method for establishing cryptographic communications that
2 are backwards compatible with preexisting public key transformation schemes, comprising the
3 step of:
4 encoding a plaintext message word M to a ciphertext word C, where M corresponds to a
5 number representative of a message and
6 $0 \leq M \leq n-1$
7 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ where k is an integer greater
8 than 2, and p_1, p_2, \dots, p_k are distinct random prime numbers, and where the ciphertext word C is
9 a number representative of an encoded form of message word M, said encoding step including
10 the steps of,
11 defining a plurality of k sub-tasks in accordance with,
12 $C_1 \equiv M^{e_1} \pmod{p_1}$,
13 $C_2 \equiv M_2^{e_2} \pmod{p_2}$,
14